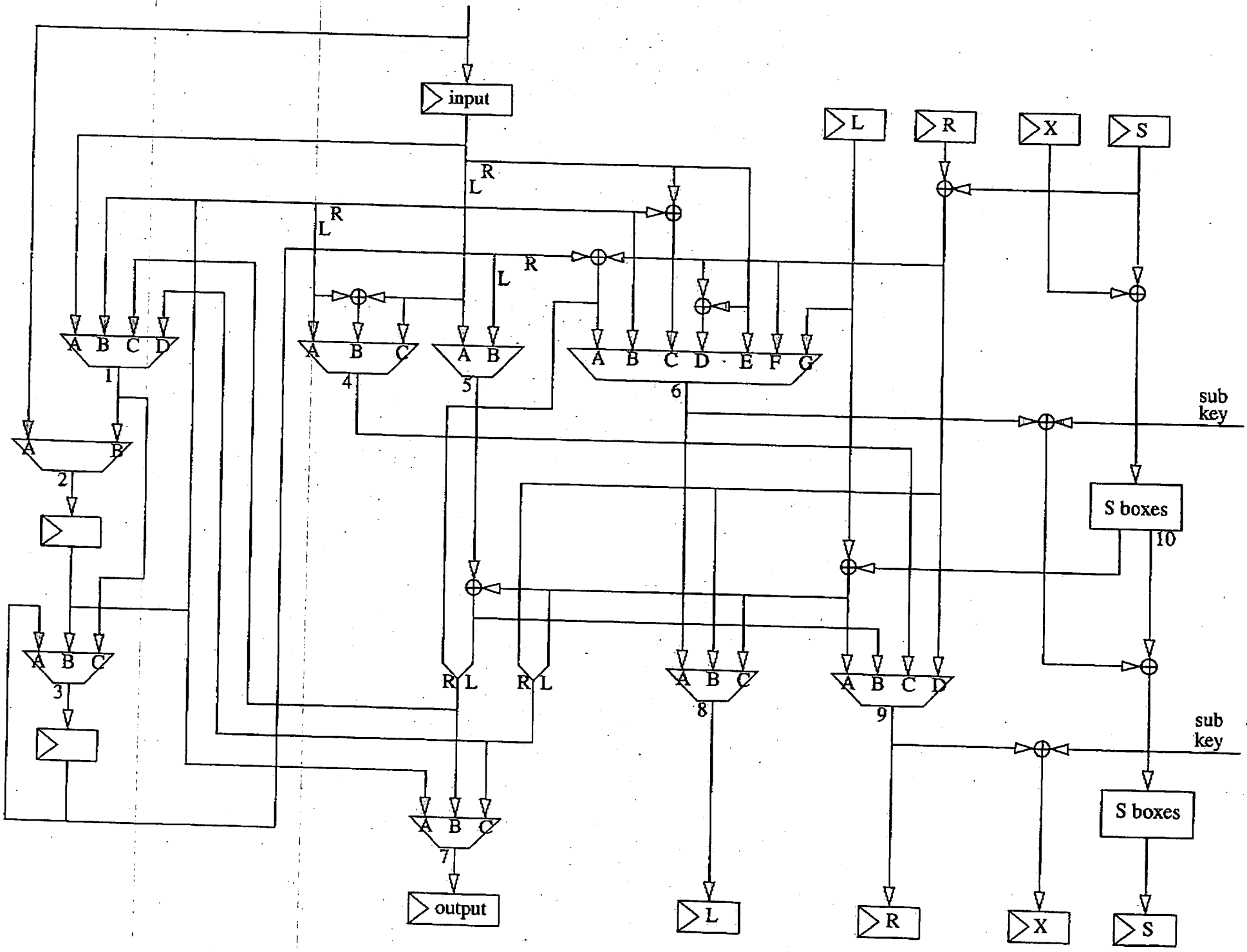
APPENDIX


input
L
R
X
S
sub key
S boxes
10
sub key
S boxes
output
L
R
X
S
A B C D
1
A B
2
A B C
3
A B C
4
A B
5
A B C D E F G
6
A B C
7
A B C
8
A B C D
9
R L
R L

Muxing for DES

item	MUX 1	2	3	4	5	6	7	8	9	Sbox
rounds 2 & 3 or 4 & 5 etc.	B	B	A	X	X	G	X	C	D	pass
triple DES rounds 16 & 1 transition	B	B	A	X	X	F	X	B	A	zero
ECB mode round 1 only	X	X	X	C	X	E	X	A	C	zero
ECB mode round 16 only	B	B	X	X	X	X	C	X	X	X
ECB mode rounds 16 & 1	X	X	X	C	X	E	C	A	C	zero
load IV	X	A	X	X	X	x	X	x	x	X
save IV	X	X	X	X	X	x	A	x	x	X
CBC mode round 1 only encrypt	X	X	X	B	X	C	X	A	C	zero
CBC mode round 1 only decrypt	A	B	B	C	X	E	X	A	C	zero
CBC mode round 16 only encrypt	D	B	X	X	X	X	C	X	X	X
CBC mode round 16 only decrypt	B	B	X	X	B	X	B	X	X	X
CBC mode rounds 16 & 1 not new IV encrypt	X	X	X	X	A	D	C	A	B	zero
CBC mode rounds 16 & 1 new IV encrypt	X	X	X	B	X	C	C	A	C	zero
CBC mode rounds 16 & 1 decrypt	A	B	B	C	B	E	B	A	C	zero

Muxing for DES

item	MUX 1	2	3	4	5	6	7	8	9	Sbox
CFB mode round 1 only encrypt	A	X	C	A	X	B	X	A	C	zero
CFB mode round 1 only decrypt	A	B	C	A	X	B	X	A	C	zero
CFB mode round 16 only encrypt	C	B	X	X	B	X	B	X	X	X
CFB mode round 16 only decrypt	B	B	X	X	B	X	B	X	X	X
CFB mode rounds 16 & 1 encrypt	A	X	C	X	B	A	B	A	B	zero
CFB mode rounds 16 & 1 decrypt	A	B	C	A	B	B	B	A	C	zero
OFB mode round 1 only	A	X	C	A	X	B	X	A	C	zero
OFB mode round 16 only	D	B	X	X	B	X	B	X	X	X
OFB mode rounds 16 & 1	A	X	C	X	B	F	B	A	A	zero